Cryptographic architectures embedded in logic devices 2023

Title: Hardware-assisted solutions to secure embedded systems on programmable logic devices

Authors: P. Brox, L. F. Rojas-Muñoz, M. C. Martínez-Rodríguez, E. Camacho, S. Sánchez-Solano

Affiliation: Instituto de Microelectrónica de Sevilla (CSIC / Univ. Sevilla)

Abstract: A mechanism to secure embedded systems implemented on programmable logic devices is the design of a hardware Root-of-Trust (RoT). The confidentiality, authentication, and integrity of data in the embedded systems rely on the RoT that is the basis to derive trust for the other layers (booting, execution environment, applications) built over it. The integration of hardware implementations for hashing, digital signature, and data encryption provides a hardened layer of protection that increases confidence in the embedded system. An additional advantage is the inclusion of a Physical Unclonable Function (PUF) in the RoT, which leverages manufacturing variations in the CMOS manufacturing process of the programmable device to extract a hardware-based fingerprint intrinsically linked to the device in which the RoT and the processing system are embedded, preventing counterfeits since the substitution with a clone will generate a completely different PUF response. Furthermore, the repeatability of the PUF output allows it to be used to infer cryptographic keys, while unpredictable phenomena affecting its basic building blocks can be exploited to infer cryptographic keys. As a proof of concept, systems-on-chip based on hard and soft core processors that include the hardware RoT were implemented on different programmable devices.